PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-036522
(43)Date of publication of application : 09.02.2001

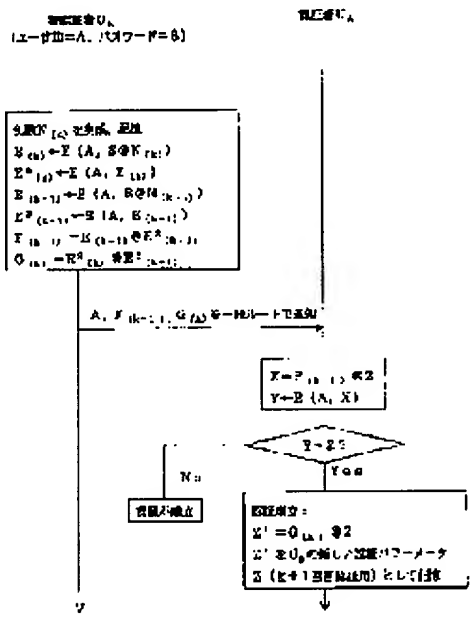
(51)Int.CI. H04L 9/32
G06F 15/00

(21)Application number : 11-207325
(22)Date of filing : 22.07.1999

(71)Applicant : NTT ADVANCED TECHNOLOGY CORP
SHIMIZU AKIHIRO
(72)Inventor : SHIMIZU AKIHIRO
KAWAMURA TORU
KURIHARA SADAMI

(54) METHOD FOR AUTHENTICATING QUALIFICATION USING VARIABLE AUTHENTICATION INFORMATION

(57)Abstract:
PROBLEM TO BE SOLVED: To realize authentication of qualification with a simple and small program size by much decreasing a processing amount executed by an authenticated party and an authentication party for each authentication phase in a qualification authentication method using variable authentication information and to provide a method for secure authentication immune to tapping on a communication line.
SOLUTION: A party to be authenticated calculates current authentication and authentication of a succeeding time by using a unidirectional function on the basis of a random number, a user ID and a password, encrypts them by applying exclusive OR to them so that other party than the party to be authenticated cannot cryptanalyze the data, transmits the result to an authentication party together with a user ID of the party to be authenticated to the authentication party. Furthermore, the authentication party receives above 3 information sets from the party to be authenticated, compares a validity confirmation parameter calculated by using the unidirectional function with the authentication parameter registered in a preceding authentication phase on the basis of the current authentication data, discriminates that the current authentication is established when they are coincident and registers the succeeding authentication data as the succeeding authentication parameter.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－36522
（P2001－36522A）
(43)公開日　平成13年２月９日(2001.2.9)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'(参考)
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７３Ａ	５Ｂ０８５
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｅ	５Ｊ１０４
		Ｈ０４Ｌ　9/00	６７３Ｃ	
			６７３Ｄ	

審査請求　未請求　請求項の数２　ＯＬ　（全 12 頁）

(21)出願番号　特願平11－207325

(22)出願日　平成11年７月22日(1999.7.22)

(71)出願人　000102739
エヌ・ティ・ティ・アドバンステクノロジ株式会社
東京都新宿区西新宿二丁目１番１号

(71)出願人　598125855
清水　明宏
高知県高知市知寄町二丁目３番地16号

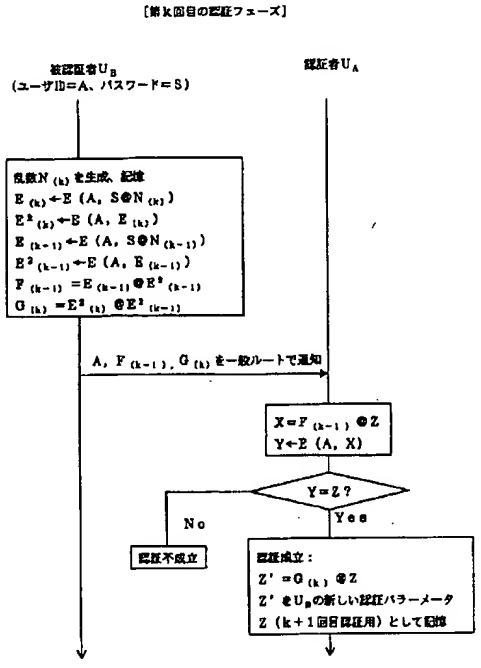
(72)発明者　清水　明宏
高知県高知市知寄町二丁目３番地16号

(72)発明者　川村　亨
東京都武蔵野市御殿山一丁目１番３号　エヌ・ティ・ティ・アドバンステクノロジ株式会社内

最終頁に続く

(54)【発明の名称】　可変認証情報を用いる資格認証方法

(57)【要約】
【課題】　可変認証情報を用いる資格認証方法において、認証フェーズ毎に被認証者側および認証者側で実行する処理量を極めて少なくすることにより、簡易で小さいプログラムサイズで実現可能とし、かつ、通信路上の盗聴に強い安全な認証を行える方法を提供する。
【解決手段】　被認証者は、乱数、ユーザＩＤ、パスワードを基に今回の認証データと次回の認証データを一方向性関数を用いて算出し、これをさらに排他的論理和を用いて被認証者以外は解読できないように暗号化し、これらを被認証者自身のユーザＩＤと合わせて認証者に送信し、また、認証者は、被認証者から前述の３つの情報を受信し、今回の認証データを基に一方向性関数を用いて算出した正当性確認パラメータと前回の認証フェーズにおいて登録した認証パラメータと比較し、一致したら今回の認証が成立したと判断し、次回の認証データを次回の認証パラメータとして登録する。



1

【特許請求の範囲】

【請求項１】被認証者が認証者に対して、被認証者が秘密に保持しているパスワードを教えることなく、自分を認証させることのできる方法で、かつ被認証者から認証者への認証依頼の度に送付する認証情報を可変とする可変認証情報を用いる資格認証方法において、

初期登録フェーズでは、

被認証者が、自己のユーザーＩＤとパスワードと乱数を基に、入力情報を算出することが計算量的に困難であるような一方向性を有する出力情報を生成する一方向性関数を用いて初回の認証データを生成する工程と、

被認証者が認証者に対して、自己のユーザーＩＤと初回の認証データを送信する工程と、

認証者が被認証者から受信した初回の認証データを初回認証時に用いる認証パラメータとして登録する工程を有し、

認証フェーズでは、

被認証者が、自己のユーザーＩＤとパスワードと乱数を基に、前記一方向性関数を用いて今回の認証データ用中間データと今回の認証データと次回の認証データを生成し、今回の認証用中間データおよび次回の認証データのそれぞれに今回の認証データで排他的論理和演算することにより、今回認証用の排他的論理和及び次回認証用の排他的論理和を生成する工程と、

被認証者が認証者に対して、自己のユーザーＩＤ、今回認証用の排他的論理和及び次回認証用の排他的論理和を送信する工程と、

認証者が、被認証者から受信した今回認証用の排他的論理和と前回登録された認証パラメータとの排他的論理和を入力情報として、前記一方向性関数を用いて被認証者の正当性確認パラメータを生成し、この正当性確認パラメータと前回登録された認証パラメータを比較し、一致した場合は認証が成立したものとし、一致しない場合は認証が不成立と判断する工程と、

認証が成立した場合は、被認証者から受信した次回認証用の排他的論理和と前回登録された認証パラメータとの排他的論理和により次回認証用の認証パラメータを生成し、前回登録された認証パラメータの替わりに前記の次回認証用の認証パラメータを登録する工程を有し、

以上の工程を順次続けて被認証者の認証を行うことを特徴とする可変認証情報を用いる資格認証方法。

【請求項２】一方向性関数ＥとしてＤＥＳ，ＦＥＡＬなどの秘密鍵暗号方式に用いる関数を用いることを特徴とする請求項第１項記載の可変認証情報を用いる資格認証方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】　本発明は、認証者が被認証者を認証する資格認証方法に関する。可変認証情報を用いる認証方法とは、被認証者から認証者への認証依頼毎

2

にパスワード等の認証情報を変更して認証を行う方法である。

【０００２】

【従来の技術】従来のパスワード等の認証情報を用いて通信相手やユーザの資格を認証する方法には、公開鍵暗号方法を応用したものと共通鍵暗号方法を応用したものの二つに大別することができるが、インタネット関連の通信プロトコルなどへの組み込みにおいては、公開鍵暗号方法より格段の高速処理が可能な共通鍵系の暗号方法を応用した方法、特に、パスワード認証方法がよく用いられる。基本的なパスワード認証の手順は以下の通りである。まず、被認証者（装置を含む）が認証者（サーバ等の装置を含む）にパスワードを登録する。認証時に、被認証者が認証者にパスワードを送信する。認証者は、受信したパスワードと登録されているパスワードを比較する。

【０００３】しかし、この方法には、次のような問題点がある。

（ａ）　認証側にあるパスワードファイルの盗見によりパスワードが盗まれる。

（ｂ）　通信中、回線盗聴によってパスワードが盗まれる。

（ｃ）　被認証者は認証者に、自分の秘密情報であるパスワードを公開する必要がある。

【０００４】最初の問題（ａ）　を解決する方法として、例えば、被認証者が認証者に、パスワードに一方向性関数を施したデータを登録しておき、認証時に、認証者が受信したパスワードに同じ一方向性関数を施し、結果を比較するという方法（参考文献：Ａ．Ｅｖａｎｓ，Ｗ．Ｋａｎｔｒｏｗｉｔｚ ａｎｄ Ｅ．Ｗｅｉｓｓ：“Ａ ｕｓｅｒ ａｕｔｈｅｎｔｉｃａｔｉｏｎ ｓｃｈｅｍｅ ｎｏｔｒｅｑｕｉｒｉｎｇ ｓｅｃｒｅｃｙ ｉｎ ｔｈｅ ｃｏｍｐｕｔｅｒ，” Ｃｏｍｍｕｎ．ＡＣＭ，１７，８，ｐｐ．４３７－４４２（１９７４）及びＲ．Ｍｏｒｒｉｓ ａｎｄ Ｋ．Ｔｈｏｍｐｓｏｎ：“Ｐａｓｓｗｏｒｄ ｓｅｃｕｒｉｔｙ：Ａ ｃａｓｅ ｈｉｓｔｏｒｙ，” ＵＮＩＸ Ｐｒｏｇｒａｍｍｅｒ’ｓ Ｍａｎｕａｌ，Ｓｅｖｅｎｔｈ Ｅｄｉｔｉｏｎ，２Ｂ（１９７９））がある。

【０００５】一方向性関数とは、入力の総当たり以外に、出力から入力を得る効率的な手段が存在しない関数であり、総当たりの計算量を充分大きくしておけば、無資格者が入力データを算出して被認証者になりすますことを防止できる。一般に、一方向性関数は、ＤＥＳやＦＥＡＬなどの共通鍵暗号方法によって得ることができる。共通鍵暗号方法は、共通秘密鍵を用いて入力される平文を処理して暗号文を出力として得るもので、平文と暗号文が与えられても共通秘密鍵が算出できない。特にＦＥＡＬでは、平文や共通秘密鍵の入力が１ビット変化

したただけでも、その入力変化の痕跡をまったくとどめない出力を得ることができるという特徴を有している。

【０００６】以上説明した通り、一方向性関数を用いた方法によって、基本的なパスワード認証方法の問題（ａ）は解決できる。しかし、これを回線盗聴が簡単なインタネットに適用する場合、問題（ｂ）　を解決することはできない。また、問題（ｃ）に関しては、この基本的なパスワード認証方法は、銀行の顧客認証などには適用できても、同一レベルのユーザ同士の資格認証には適していない。

【０００７】このような問題を解決する方法として、パスワード等の認証情報を可変にする資格認証方法がある。例えば、Ｌａｍｐｏｒｔ　の方法（Ｌ．Ｌａｍｐｏｒｔ：“Ｐａｓｓｗｏｒｄ　ａｕｔｈｅｎｔｉｃａｔｉｏｎ　ｗｉｔｈ　ｉｎｓｅｃｕｒｅ　ｃｏｍｍｕｎｉｃａｔｉｏｎ，”　Ｃｏｍｍｕｎ．　ＡＣＭ，　２４，１１，　ｐｐ．７７０－７７２（１９８１））　（Ｓ／ＫＥＹ型パスワード認証方式）及びこの出願の発明者が提案した動的パスワード認証方法　であるＣＩＮＯＮ法（Ｃｈａｉｎｅｄ　Ｏｎｅ－ｗａｙ　Ｄａｔａ　ＶｅｒｉｆｉｃａｔｉｏｎＭｅｔｈｏｄ）（Ａ．Ｓｈｉｍｉｚｕ，　“ＡＤｙｎａｍｉｃ　Ｐａｓｓｗｏｒｄ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｍｅｔｈｏｄ　Ｕｓｉｎｇ　ａ　Ｏｎｅ－ｗａｙ　Ｆｕｎｃｔｉｏｎ”Ｓｙｓｔｅｍｓ　ａｎｄ　Ｃｏｍｐｕｔｅｒｓｉｎ　Ｊａｐａｎ，　Ｖｏｌ．　２２，　Ｎｏ．７，　１９９１，　ｐｐ．３２－４０）（「資格認証方法」　特公平８－２０５１／特許第２０９８２６７号）がある。

【０００８】Ｌａｍｐｏｒｔ　の方法は、パスワードに一方向性関数を複数回適用しておいて、適用一回前のデータを次々と認証者側に示すことで、複数回の認証を可能にする方法である。この方法では、最初に設定した最大認証回数から認証を実行する毎に１を減算し、認証回数を使い尽くした時点で、パスワードを再設定する必要がある。最大認証回数を増やすために一方向性関数の適用回数を増加させると処理量が増大する。銀行の顧客認証では最大認証回数として数１００～１０００等が用いられる。更に、認証者側に比較して処理能力の小さい、被認証者側の処理負担が大きいという問題点がある。

【０００９】ＣＩＮＯＮ法は、被認証者（ユーザ）が認証者（ホスト）に対して、前回に正当性の検証を終え登録されている認証データのもとのデータ、次々回に認証に用いる認証データ、前回送信済みで次回の認証に用いる認証データの正当性検証データの３つのデータを認証フェーズ毎に送信することで、認証情報を安全に更新しながら次々と連鎖的に認証を行うことのできる方法である。このように、ＣＩＮＯＮ法では、被認証者が認証者の認証を得るためには、前回生成した２つの乱数$N_{(k-1)}$，$N_{(k)}$を使用する必要がある。そのため、ユーザが出先の端末から認証者の認証を得る場合には、ユーザはそれらの乱数を記憶した例えばＩＣカードの様な記憶媒体を携帯し、出先の端末で使用しなければならない。また、端末は、乱数を発生する機能及びＩＣカードを読み書きする機能を必要とする。一方、インタネットにおいては、テレビセットやワードプロセッサ、更に携帯端末などにインタネット接続機能を付加したインタネット家電と呼ばれる製品が市場投入されようとしている。

【００１０】このようなインタネット家電が普及してくることに伴い、認証処理を有する情報の送受信に対する需要が増大してくるものと思われるが、インタネット家電は、コストを最重視しているため、上述の乱数を発生したり、それらをＩＣカード等の記憶媒体へ読み書きする機構を有していない場合がほとんどである。また、処理プログラムの格納領域も限られるため、このような認証処理をできるだけ簡易で小さいプログラムサイズで実現することが望まれる。

【００１１】この問題を解決するために、本出願の発明者が提案した「ユーザ認証機能を有する情報送受信制御方法」（特願平８－２４０１９０）におけるユーザ認証方式は、インターネット等のセキュリティが十分でないネットワーク上の被認証者と認証者間の情報送受信において、被認証者側にＩＣカード等の記憶媒体の読み書きを行う機構を必要とせず、かつユーザ認証処理を小さいプログラムサイズで行うことができる安全な情報送受信制御方法と装置及びその方法を記録した記録媒体を提供することを目的としたもので、認証手順において、ＣＩＮＯＮ法の改良として、各種認証データの値を一度きりのものにするために被認証ユーザと認証サーバとの間で同期をとらなくてはならないパラメータとして、認証データ生成時に用いていた乱数に代えて、認証回数を用いるようにしたことを主要な特徴とする。被認証ユーザが行わなければならない処理が上記「資格認証方法」よりもややシンプルになっている。この発明においては、認証データの生成に用いる一方向性関数にＤＥＳやＦＥＡＬなどの共通鍵暗号方法を用いる。しかるに、安全性は用いる一方向性関数、つまり共通鍵暗号方法の強度に依存し、乱数から認証回数に変更した影響はない。

【００１２】上記３方式における認証方法は全て可変認証情報を用いる資格認証方法である。かかる資格認証方法の重要な特徴は、インターネット等の通信路を通して被認証者から認証者に渡される認証用データは認証フェーズ毎に異なる（毎回異なる）ため、ある認証フェーズでそれが盗聴されたとしても、次の認証フェーズ（次回認証時）には別の認証データを被認証者から認証者に送らなければ認証されないので、盗聴した無資格者が正当な被認証者になりすますことができないという点である。

【００１３】

【発明が解決しようとする課題】Ｌａｍｐｏｒｔの方法には、被認証ユーザ側での処理（計算）量が非常に大き

いという問題と、被認証者が、定期的にパスワードを更新する必要があるという問題があった。ＣＩＮＯＮ法では、Ｌａｍｐｏｒｔの方法の欠点であるパスワードの更新の必要性をなくすことができたが、被認証者および認証者における処理（計算）量が大きいという問題は依然残った。「ユーザ認証機能を有する情報送受信制御方式」におけるユーザ認証方法は、ＣＩＮＯＮ法の欠点である、被認証者における処理（計算量）を削減することができたが、被認証者と認証者の相互間の手順がやや複雑であり、認証サーバ側でユーザ対応に管理しなければならないデータが多く、実運用時には準正常系、異常系の処理手順を入念に検討しておく必要があるという問題があった。

【００１４】本発明の目的は、セキュリティが十分でないネットワーク上の被認証者を認証者に認証させるための可変認証情報を用いる資格認証方法において、認証フェーズ毎に被認証者側および認証者側で実行する処理量（計算量）を極めて少なくすることにより、被認証側にも認証側にも簡易で小さいプログラムサイズで実現可能とし、かつ、通信路上の盗聴に強い安全な認証を行える方法を提供することにある。

【００１５】

【課題を解決するための手段】上記課題を解決するために、本発明による可変認証情報を用いる資格認証方法は、被認証者が認証者に対して、被認証者が秘密に保持しているパスワードを教えることなく、自分を認証させることのできる方法で、かつ被認証者から認証者への認証依頼の度に送信する認証情報を可変とする資格認証方法において、初期登録フェーズでは、被認証者が、自己のユーザーＩＤとパスワードと乱数を基に、入力情報を算出することが計算量的に困難であるような一方向性を有する出力情報を生成する一方向性関数を用いて初回の認証データを生成する工程と、被認証者が認証者に対して、自己のユーザーＩＤと初回の認証データを送信する工程と、認証者が被認証者から受信した初回の認証データを初回認証時に用いる認証パラメータとして登録する工程を有し、認証フェーズでは、被認証者が、自己のユーザーＩＤとパスワードと乱数を基に、前記一方向性関数を用いて今回の認証データ用中間データと今回の認証データと次回の認証データを生成し、今回の認証用中間データおよび次回の認証データのそれぞれに今回の認証データで排他的論理和演算することにより、今回認証用の排他的論理和及び次回認証用の排他的論理和を生成する工程と、被認証者が認証者に対して、自己のユーザーＩＤ、今回認証用の排他的論理和及び次回認証用の排他的論理和を送信する工程と、認証者が、被認証者から受信した今回認証用の排他的論理和と前回登録された認証パラメータとの排他的論理和を入力情報として、前記一方向性関数を用いて被認証者の正当性確認パラメータを生成し、この正当性確認パラメータと前回登録された認証パラメータを比較し、一致した場合は認証が成立したものとし、一致しない場合は認証が不成立と判断する工程と、認証が成立した場合は、被認証者から受信した次回認証用の排他的論理和と前回登録された認証パラメータとの排他的論理和により次回認証用の認証パラメータを生成し、前回登録された認証パラメータの替わりに前記の次回認証用の認証パラメータを登録する工程を有し、以上の工程を順次続けて被認証者の認証を行うことを特徴とする。

【００１６】すなわち、本発明は、被認証者（装置を含む）は、認証フェーズ毎に乱数を生成し、乱数、ユーザＩＤ、パスワードを基に今回の認証データと次回の認証データを一方向性関数を用いて算出し、これをさらに排他的論理和を用いて被認証者以外は解読できないように暗号化し、これらを被認証者自身のユーザＩＤと合わせて認証者（サーバ等の装置を含む）に送信し、また、認証者は、被認証者から前述の３つの情報を受信し、今回の認証データを基に一方向性関数を用いて算出した正当性確認パラメータと前回の認証フェーズにおいて登録した認証パラメータと比較し、一致したら今回の認証が成立したと判断し、次回の認証データを次回の認証パラメータとして登録するものである。

【００１７】これにより、本発明は、（１）前記の従来技術において１回の認証処理実行時に、被認証者と認証者との間で行われる認証関連情報の授受が、被認証者からみて１往復半（計３回の送受信）以上必要であったのが、被認証者が認証者に対して１回の送信のみですむようになった、（２）前記の従来技術において認証者が被認証者毎に管理している認証関連データが４以上あったのに対して、本方式ではわずか１のデータのみですむようになった、（３）認証フェーズ毎に被認証者側および認証者側で排他的論理和演算以外の暗号化又は複合処理が認証側で２回、被認証者側で４回と少なくなった、ことにより被認証者および認証者が実行する処理量（計算量）を極めて少なくすることができるという主要な効果を有する。

【００１８】また、一方向性関数ＥとしてＤＥＳ，ＦＥＡＬなどの秘密鍵暗号方式に用いる関数を用いるのが好適である。認証情報の解読が不可能であり、さらに、ＦＥＡＬは高速暗号処理を実現している。

【００１９】

【発明の実施の形態】

【実施例１】本発明による可変認証情報を用いる資格認証方法の説明に先だって、まず一方向性関数について説明する。一方向性関数とは、入力データのしらみ潰し以外に、出力データから入力データを逆算する有効な方法のない関数をいう。ＤＥＳ、ＦＥＡＬなどの秘密鍵暗号アルゴリズムを用いて、このような性質を実現できる。特に、ＦＥＡＬは、１６ビットのパーソナルコンピュータ上のソフトウェアで２００Ｋｂｐｓ、ＬＳＩとして９

６Ｍｂｐｓ（クロック１０ＭＨｚ）の暗号化処理速度を実現しているすぐれた秘密鍵暗号方式である。

【００２０】秘密鍵暗号アルゴリズムをＣ＝Ｅ（P_A，S_B）で表す。Ｅは一方向性関数（秘密鍵暗号化処理関数、第２パラメータが秘密鍵）で、Ｃは暗号文、P_Aは平文、S_Bは秘密鍵である。P_Aを平文、S_Bを入力情報、Ｃを出力情報とすると、平文P_Aと出力情報Ｃが分かっていても入力情報S_Bを逆算できない。

【００２１】続いて本発明の資格認証方法の実施例を説明する。本発明の認証方法のデータの流れを図１ないし図３に示す。図１は初期登録フェーズ、図２は初回認証フェーズ、図３はｋ回目認証フェーズのデータの流れを示す。データは上から下に又は矢印に沿って流れる。図及び以下の説明において、一方向演算Ｃ＝Ｅ（P_A，S_B）をＣ←Ｅ（P_A，S_B）のように表す。また、排他的論理和演算子を＠で表す。

【００２２】図４は本発明の資格認証方法を実現する機能ブロックの実施例を示す。図４において、１は認証制御機構、２は被認証制御機構、３は公開簿、４は秘密情報入力機構、５は乱数生成機構、６は一方向性情報生成機構、７は乱数記録機構、８は情報送信機構、９は情報受信機構、１０は情報記録機構、１１は情報比較機構、１２は演算機構である。本実施例では、認証者U_Aを認証サーバ、被認証者U_Bを被認証ユーザとし、その認証手順を示す。被認証ユーザU_BはP_Aとして公開された自己のユーザＩＤ＝Ａを持ち、自分のみで秘密に管理するパスーワードＳを持つものとし、S_BとしてパスーワードＳと乱数との排他的論理和を用いるものとする。

【００２３】本実施例における認証方法は、大きく分けて、初期登録フェーズとその後の認証フェーズの２つのフェーズから成り立つ。認証フェーズは第１回目、第２回目、第３回目…と順次繰り返される。認証サーバU_Aの認証制御は認証制御機構１が行う。また、被認証ユーザU_Bの被認証制御は被認証制御機構２が行う。また、上記ユーザＩＤ　Ａは公開簿３に登録されている。

【００２４】［初期登録フェーズ］まず、初期登録フェーズについて説明する。

①被認証ユーザU_B側（演算処理）

パスワードＳは秘密情報入力機構４によって取り込まれる。自分のユーザＩＤとしてP_A＝Ａを用いる。$N_{(0)}$を乱数生成機構５によって任意に設定し、乱数記録機構７によって記録しておく。一方向性情報生成機構６によって以下のデータを算出する。一方向性関数として秘密鍵暗号化処理関数Ｅを用いる。まず、初回の認証用中間データ　$E_{(0)}$←Ｅ（Ａ，Ｓ＠$N_{(0)}$）を生成し、更に、初回の認証データ　$E^2_{(0)}$←Ｅ（Ａ，$E_{(0)}$）を生成する。

【００２５】②被認証ユーザU_B側（送信処理）

以上の準備をした上で、情報送信機構８によって認証サーバU_Aに以下のデータを送信し、登録を依頼する。この場合、盗聴の恐れのないセキュアルート（安全なルート）により送信する。ユーザＩＤ　Ａ，初回の認証データ　$E^2_{(0)}$

【００２６】③認証サーバU_A側（受信、登録処理）

情報受信機構９でユーザＩＤ　Ａおよび初回の（次回の）認証データ$E^2_{(0)}$を受信し、受信したデータ$E^2_{(0)}$を情報記録機構１０で初回の認証パラメータ（認証パラメータ初期値）Ｚとして記憶（登録）する。

【００２７】［認証フェーズ］次に、認証フェーズについて説明する。まず、初回（ｋ＝１）の認証手順について説明する。①被認証ユーザU_B側（演算処理）

乱数生成機構５によりN_1を任意に設定し、乱数記録機構７に記憶させる。次に、一方向性情報生成機構６によって以下のデータを算出する。次回の認証用中間データ　$E_{(1)}$←Ｅ（Ａ，Ｓ＠$N_{(1)}$）を生成し、更に、次回の認証データ　$E^2_{(1)}$←Ｅ（Ａ，$E_{(1)}$）を生成する。次に、初期登録フェーズで乱数記録機構７に記憶させた$N_{(0)}$を使って、今回の認証用中間データ　$E_{(0)}$←Ｅ（Ａ，Ｓ＠$N_{(0)}$）を生成し、更に、今回の認証データ　$E^2_{(0)}$←Ｅ（Ａ，$E_{(0)}$）を生成する。次に、演算機構１２によって以下のデータを算出する。今回認証用の排他的論理和　$F_{(0)}=E_{(0)}$＠$E^2_{(0)}$を算出し、更に、次回認証用の排他的論理和　$G_{(1)}=E^2_{(1)}$＠$E^2_{(0)}$を算出する。

【００２８】②被認証ユーザU_B側（送信処理）

情報送信機構８によって認証サーバU_Aに以下のデータを送信する。ユーザＩＤ　Ａ，今回認証用の排他的論理和$F_{(0)}$，次回認証用の排他的論理和$G_{(1)}$この時、送信データは被認証者以外は解読できないように暗号化されているので、インターネットのような盗聴の恐れのあるルート（一般ルート）を用いてもよい。

【００２９】③認証サーバU_A側（受信、認証処理）

ユーザＩＤ　Ａ，今回認証用の排他的論理和$F_{(0)}$，次回認証用の排他的論理和$G_{(1)}$を受信し、次に、正当性確認用中間パラメータＸを、演算機構１２にて以下の演算により生成する。

$X=F_{(0)}$＠Ｚ

ここで、$Z=E^2_{(0)}$は初期登録フェーズで情報記録機構１０に登録された認証パラメータである。この排他的論理和演算処理において、$F_{(0)}=E_{(0)}$＠$E^2_{(0)}$が正当な被認証ユーザU_Bから受信したものであれば、演算結果は$X=E_{(0)}$になるはずである。　次に、正当性確認パラメータＹを一方向性情報生成機構６にて以下の演算により生成する。

Ｙ←Ｅ（Ａ，Ｘ）

もし、正当性確認パラメータＹと初期登録フェーズで記憶（登録）された認証パラメータ$Z=E^2_{(0)}$が一致すれば、今回の認証が成立したことになり、一致しなければ認証は不成立となる。

【００３０】④認証サーバU_A側（登録処理）

認証が成立した場合には、次回の認証パラメータZ'を演算機構１２にて以下の演算により生成する。以下、認証パラメータZ，Z'について、受信データをもとに演算して得られたものをZ'、登録されたものをZと切り分けて用いる。

$Z' = G_{(1)} @ Z$

ここで、$Z = E^{2}_{(0)}$は初期登録フェーズで情報記録機構１０に登録された認証パラメータであり、$G_{(1)} = E^{2}_{(1)} @ E^{2}_{(0)}$は被認証ユーザ$U_B$から受信したデータである。既に認証が成立しているため、$G_{(1)}$はユーザＩＤ＝Ａの被認証ユーザから正当に受信したものであり、演算結果は$Z' = E^{2}_{(1)}$になるはずである。最後に、$Z' = E^{2}_{(1)}$を、次回すなわち第２回目の認証で用いる認証パラメータZとして情報記録機構１０に記憶（登録）する。認証が不成立の場合には、認証パラメータZは不変である。

【００３１】一般に、第ｋ回目（ｋは正整数）の認証手順は以下の通りである。

①被認証ユーザU_B側（演算処理）

乱数生成機構５により$N_{(k)}$を任意に設定し、乱数記録機構７に記憶させる。一方向性情報生成機構６によって以下のデータを算出する。次回の認証用中間データ　$E_{(k)} \leftarrow E(A, S @ N_{(k)})$を生成し、更に、次回の認証データ　$E^{2}_{(k)} \leftarrow E(A, E_{(k)})$を生成する。次に、前回の認証フェーズで乱数記録機構７に記憶させた$N_{(k-1)}$を使って、今回の認証用中間データ　$E_{(k-1)} \leftarrow E(A, S @ N_{(k-1)})$を生成し、更に、今回の認証データ　$E^{2}_{(k-1)} \leftarrow E(A, E_{(k-1)})$を生成する。次に、演算機構１２によって以下のデータを算出する。今回認証用の排他論理和　$F_{(k-1)} = E_{(k-1)} @ E^{2}_{(k-1)}$を算出し、更に、次回認証用の排他論理和　$G_k = E^{2}_{(k)} @ E^{2}_{(k-1)}$を算出する。

【００３２】②被認証ユーザU_B側（送信処理）

情報送信機構８によって認証サーバU_Aに以下のデータを送信する。ユーザＩＤ　Ａ，今回認証用の排他論理和$F_{(k-1)}$，次回認証用の排他論理和$G_{(k)}$この時、送信データは被認証者以外は解読できないように暗号化されているので、インターネットのような盗聴の恐れのあるルート（一般ルート）を用いてもよい。

【００３３】③認証サーバU_A側（受信、認証処理）

ユーザＩＤ　Ａ，今回認証用の排他論理和$F_{(k-1)}$，次回認証用の排他論理和$G_{(k)}$を受信し、次に、正当性確認用中間パラメータXを演算機構１２にて以下の演算により生成する。

$X = F_{(k-1)} @ Z$

ここで、$Z = E^{2}_{(k-1)}$は前回の認証フェーズで情報記録機構１０に登録された認証パラメータを用いる。この排他的論理和演算処理において、$F_{(k-1)}$が正当な被認証ユーザU_Bから受信したものであれば、演算結果は$X = E_{(k-1)}$になるはずである。　次に、正当性確認パラメータYを一方向性情報生成機構６にて以下の演算により生成する。

$Y \leftarrow E(A, X)$

もし、正当性確認パラメータYと前回の認証フェーズで登録された認証パラメータ$Z = E^{2}_{(k-1)}$が一致すれば、今回の認証が成立したことになり、一致しなければ認証は不成立となる。

【００３４】④認証サーバU_A側：認証が成立した場合には、次回の認証パラメータZ'を演算機構１２にて以下の演算により生成する。

$Z' = G_{(k)} @ Z$

ここで、$Z = E^{2}_{(k-1)}$は前回の認証フェーズで情報記録機構１０に登録された認証パラメータであり、$G_{(k)} = E^{2}_{(k)} @ E^{2}_{(k-1)}$は被認証ユーザ$U_B$から受信したデータである。既に認証が成立しているため、$G_{(k)}$はユーザＩＤ＝Ａの被認証ユーザから正当に受信したものであり、演算結果は$Z' = E^{2}_{(k)}$になるはずである。最後に、$Z' = E^{2}_{(k)}$を、ユーザＩＤ＝Ａの被認証ユーザが次回の認証で用いる新たな認証パラメータZとして情報記録機構１０に記憶（登録）する。認証が不成立の場合には、認証パラメータZは不変である。以上の認証フェーズをｋ＝１，２，３，…と順次続けて、被認証者のパスワードの認証を行う。

【００３５】本実施例による資格認証方法の効果は、次のようである。第ｋ回目の認証フェーズで、被認証ユーザU_Bが認証サーバU_Aに送信する今回認証用の排他論理和$F_{(k-1)}$および次回認証用の排他論理和$G_{(k)}$は、一方向性関数を用いて生成した$E^{2}_{(k-1)}$との排他的論理和演算により一種の暗号化が施されているため、第３者に不正に盗聴されても実データを解読することはできない。

【００３６】第ｋ回目の認証フェーズで、認証サーバU_Aが被認証ユーザU_Bから受信した今回認証用の排他論理和$F_{(k-1)}$および次回認証用の排他論理和$G_{(k)}$は、それぞれ認証パラメータ$Z = E^{2}_{(k-1)}$との排他的論理和演算により一種の暗号化が施されているが、$E^{2}_{(k-1)}$は、前回認証フェーズ（ｋ＝１の場合は初期登録フェーズ）において認証サーバU_Aに既に登録されているものであるため、$E^{2}_{(k-1)}$と再度排他的論理和演算することによって極めて簡単に、正当性認証用中間パラメータ$X = E_{(k-1)}$と次回の認証パラメータ$Z = E^{2}_{(k)}$を復号することができる。排他的論理和演算は演算処理負荷が最もシンプルな一方向性関数の一つであり、かつ、２度演算すると元のデータを復元できるという特徴を持つ。

【００３７】認証サーバ側において、被認証ユーザ毎に記憶（管理）しておかなければならないデータは、上記の認証パラメータ$Z = E^{2}_{(k-1)}$のわずか１つだけであり、認証フェーズ毎に認証サーバ内で実行しなくてはならない排他的論理和演算以外の復号処理（一方向性関数の使用）はわずか２回（正当性認証パラメータY，認証パラメータZの生成）であり、処理負荷を極めて軽くす

ることができる。

【００３８】被認証ユーザ側において、認証フェーズ毎に実行しなくてはならない排他的論理和演算以外の暗号化処理（一方向性関数の使用）は４回（今回の認証用中間データ$E_{(k-1)}$，今回の認証データ$E'_{(k-1)}$，次回の認証用中間データ$E_{(k)}$，次回の認証データ$E'_{(k)}$）であり、処理負荷は十分に軽くてすむ。

【００３９】被認証ユーザと認証サーバの相互間で行われる情報授受の回数は、認証フェーズ毎に、被認証ユーザから認証サーバへの送信が１回のみであるため、通信セッション（コネクション）の状態が不安定なネットワークにおいても確実に認証処理を行うことができる。

【００４０】

【実施例２】実施例１では、第ｋ回目の認証フェーズで、被認証ユーザU_B側で、乱数生成機構５により$N_{(k)}$を任意に設定し、乱数記録機構７に記憶させることになっているが、本実施例では、$N_{(k)}$に代えて、$E_{(k)}$および$E'_{(k)}$を記憶しておく。これにより、認証フェーズ毎に被認証ユーザU_B側で実行しなくてはならない排他的論理和演算以外の暗号化処理をわずか２回に削減することができる。

【００４１】以上の手順では、登録フェーズで認証者が記憶する初回認証データは$E'_{(0)}$であるが、安全性をより高めるために、一方向性関数を利用する回数を増やし、$E'_{(0)}$の代わりに初回認証データとして、$Z_{(0)}=E_{(0)}\leftarrow E(A, E'_{(0)})$を記憶させ、第ｋ回目の認証フェーズでは、被認証者は認証者に対してユーザＩＤ　Ａ、今回認証用の排他的論理和$F_{(k-1)}=E'_{(k-1)}@E_{(k-1)}$、次回認証用の排他的論理和$G_{(k)}=E_{(k)}@E_{(k-1)}$（ここに$E'_{(k-1)}$は今回認証用中間データ、$E_{(k-1)}$は今回の認証データ、$E_{(k)}$は次回の認証データである。）を送り、それを受信した認証者は、記憶していた認証パラメータ$Z=E_{(k-1)}$から今回認証用中間データ$E'_{(k-1)}$と次回の認証データ$E_{(k)}$を復元し、得られた$E'_{(k-1)}$とユーザＩＤ　Ａから正当性確認パラメータ$Y=E_{(k-1)}$を生成して、記憶していた認証パラメータ$Z=E_{(k-1)}$と比較することで認証し、認証成立した場合には$E_{(k)}$を次回認証パラメータＺとして記憶するいう手順を採ることも可能である。または、ユーザＩＤ　Ａ、今回認証用の排他的論理和$F_{(k-1)}=E_{(k-1)}@E_{(k-1)}$、次回認証用の排他的論理和$G_{(k)}=E_{(k)}@E_{(k-1)}$を送り（ここに$E_{(k-1)}$は今回認証用中間データ、$E_{(k-1)}$は今回の認証データ、$E_{(k)}$は次回の認証データである。）、それを受信した認証者は、記憶していた認証パラメータ$Z=E_{(k-1)}$から今回認証用中間データ$E_{(k-1)}$とユーザＩＤ　Ａから正当性確認パラメータ$Y=E_{(k-1)}$を生成して、記憶していた$Z=E_{(k-1)}$と比較することで認証し、認証成立した場合には$E_{(k)}$を次回認証データとして記憶するいう手順を採ることも可能である。さらに、登録フェーズで認証者に記憶させる初回認証データを、$E'_{(0)}=E(A, E_{(0)})$やや$E_{(0)}=E(A, E'_{(0)})$などとする手順も可能である。

【００４２】以上の実施例では、認証サーバU_Aと被認証ユーザU_Bとの間の資格認証方法について説明したが、インターネット利用者同士の資格認証にも本発明を適用できる。その他、本発明の趣旨を逸脱しない範囲で種々の変更が可能なことはいうまでもない。

【００４３】

【発明の効果】以上説明したように、本発明による可変認証情報を用いる資格認証方法は、被認証側が認証側に対して送信するデータは一方向性関数を用いて算出し、これをさらに排他的論理和を用いて被認証者以外は解読できないように暗号化しているので、自分の秘密情報を相手に示すことなく、さらに使い捨てでない資格認証方式を実現できる。また、不正行為者が通信中の認証情報を自分に都合のいいものに改ざんしたとしても、その正当性を保証できないので次回の認証は受けられない。

【００４４】また、実施例で示した認証手順では、認証される側の一方向性情報生成処理は、一回の認証につき２～４回で済む。これはＬａｍｐｏｒｔの方式の数１００～１０００回に比べて著しく小さい。また、ＣＩＮＯＮ法においても１回の認証処理実行時に、被認証者と認証者との間で行われる認証関連情報の授受が、被認証者からみて１往復半（計３回の送受信）必要であったのが、本発明では被認証者から認証者に対する１回の送信のみですむようになった。

【００４５】さらに、従来技術において認証者が被認証者毎に管理している認証関連情報が４種類あったのに対して、本方式ではわずか１の情報のみですむようになった。

【００４６】このように、本発明は、特に、認証フェーズ毎に被認証者側および認証者側で実行する処理量（計算量）を極めて少なくすることができる。したがって、セキュリティが十分でないネットワーク上の被認証者を認証者に認証させるための認証方法として、被認証側にも認証側にも簡易で小さいプログラムサイズで実現可能な処理しかさせず、かつ、通信路上の盗聴に強い安全な認証を行える方法を提供することができる。

【００４７】本発明の可変認証情報を用いる資格認証方法は、ネットワーク、通信、コンピュータシステムにおけるあらゆる状況の資格認証に適用することができる。例えば、認証される側の処理量が少なく済むため、ＩＣカードの認証システムに適用することができる。これを応用して、ＩＣカード電話機などのシステムに適用できる。また、ネットワーク上の同一レベルのユーザ同士の相互認証に適用できる。データベースの情報へのアクセス資格の認証へ適用できる。さらに、利害関係の異なるユーザグループが同一のＬＡＮ上に共存しているような場合の、それぞれのグループの情報へのアクセス資格の認証への適用も可能である。この場合には、かなりの高

速性が要求されるので、一方向性変換処理を実現する秘密鍵暗号はＬＳＩを用いることが必要である。

【図面の簡単な説明】

【図１】本発明における資格認証方法（初期登録フェーズ）の実施例を示す図である。

【図２】本発明における資格認証方法（初回認証フェーズ）の実施例を示す図である。

【図３】本発明における資格認証方法（ｋ回目認証フェーズ）の実施例を示す図である。

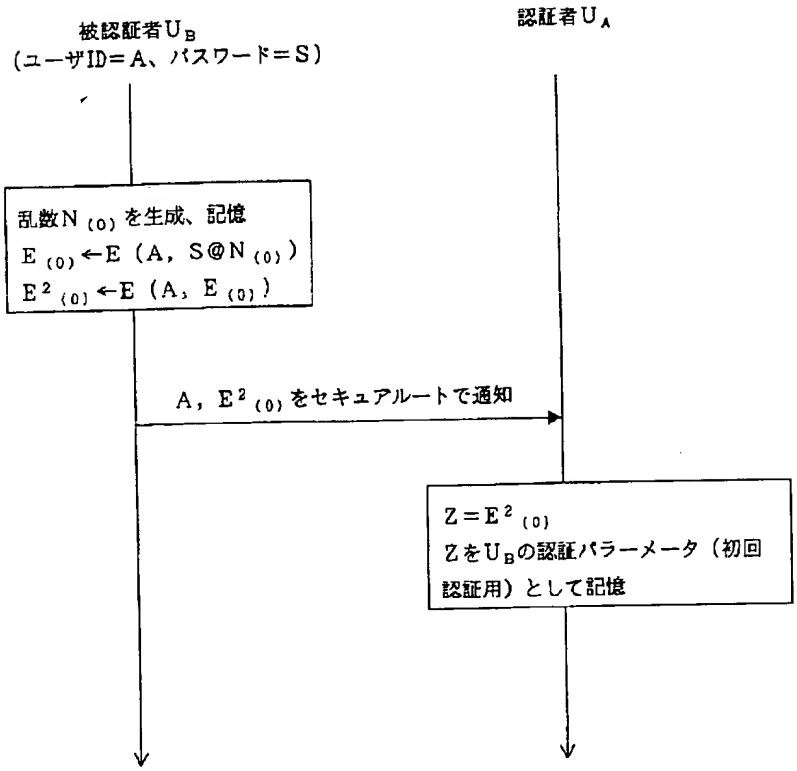
【図４】本発明における機能ブロックの実施例を示す図である。

【符号の説明】

1　認証制御機構
2　被認証制御機構
3　公開簿
4　秘密情報入力機構
5　乱数生成機構
6　一方向性情報生成機構
7　乱数記録機構
8　情報送信機構
9　情報受信機構
１０　情報記録機構
１１　情報比較機構
１２　演算機構
A　ユーザＩＤ
C　出力情報
E　一方向性関数（秘密鍵暗号化処理関数、第２パラメータが秘密鍵）
$E^2_{(k-1)}$　今回認証用データ
$E^2_{(k)}$　次回認証用データ
$F_{(k-1)}$　今回認証用の排他論理和
$G_{(k)}$　次回認証用の排他論理和
$N_{(k)}$　乱数
P_A　平文
S　パスワード
S_B　入力情報（秘密鍵）
U_A　認証者（装置を含む）
U_B　被認証者（装置を含む）
X　正当性確認用中間パラメータ
Y　正当性確認パラメータ
Z　認証パラメータ（登録されたもの）
Z'　次回の認証パラメータ（受信データをもとに演算して得られたもの）

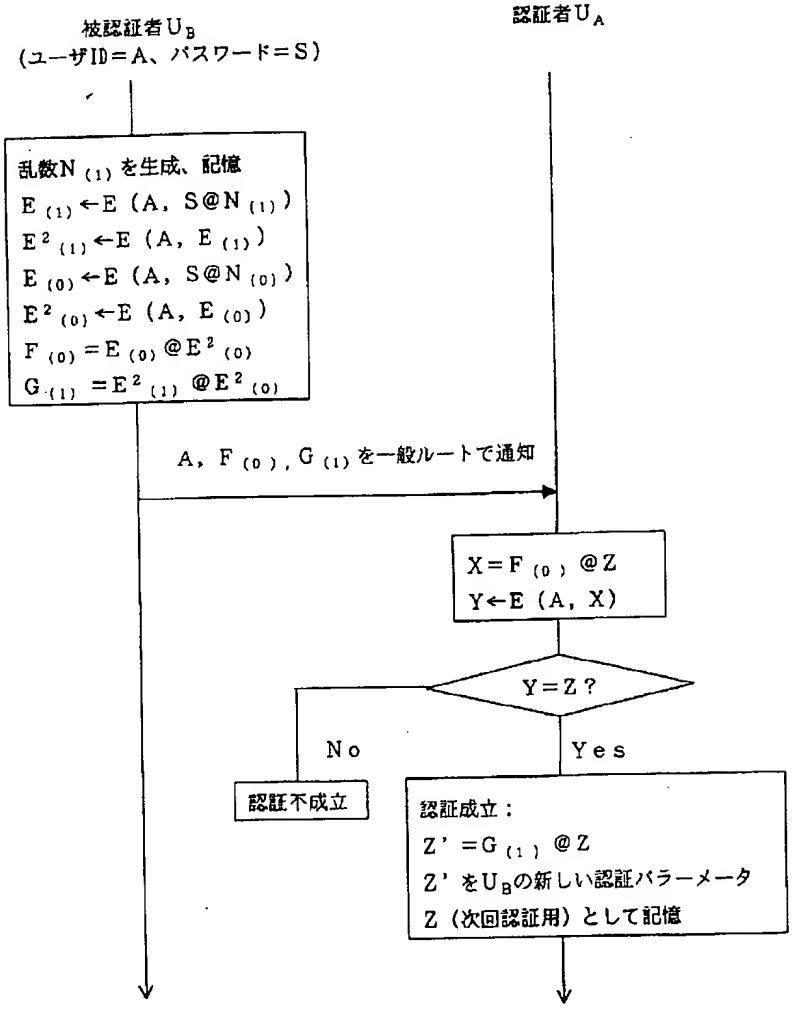
【図１】

［登録フェーズ］


被認証者U_B
(ユーザID＝A、パスワード＝S)
認証者U_A
乱数$N_{(0)}$を生成、記憶
$E_{(0)} \leftarrow E(A, S@N_{(0)})$
$E^2_{(0)} \leftarrow E(A, E_{(0)})$
A，$E^2_{(0)}$をセキュアルートで通知
$Z = E^2_{(0)}$
ZをU_Bの認証パラーメータ（初回認証用）として記憶

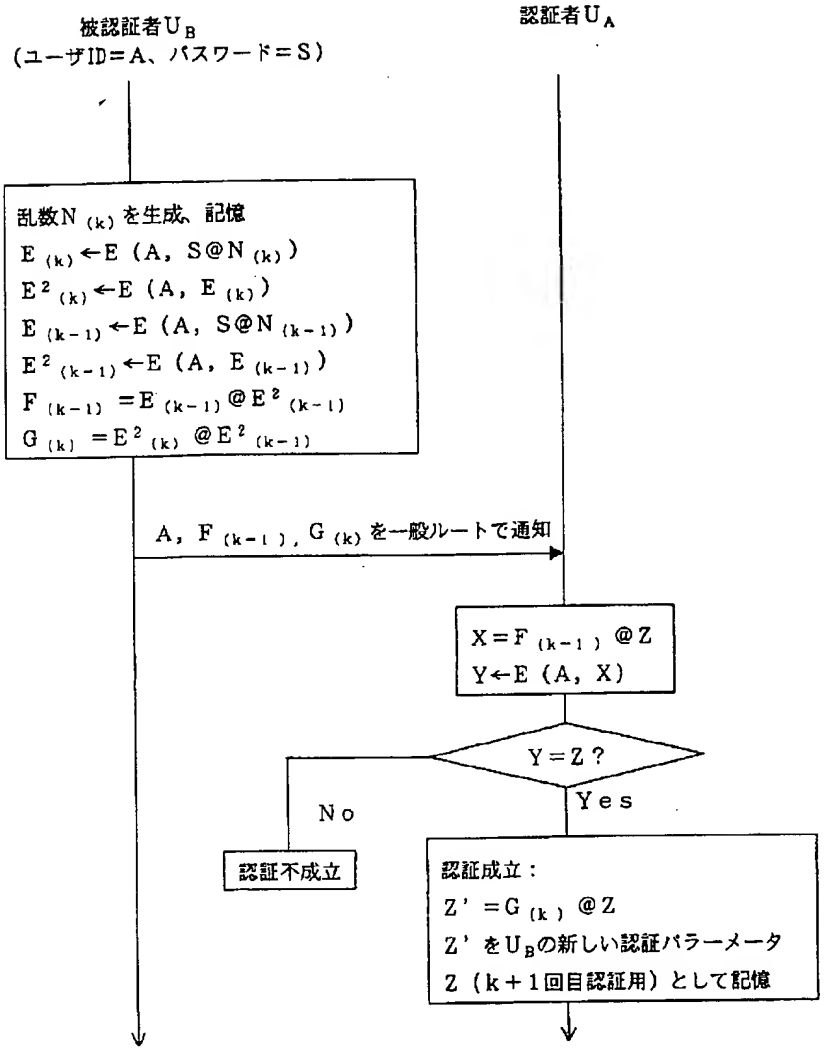
【図２】

［初回認証フェーズ］

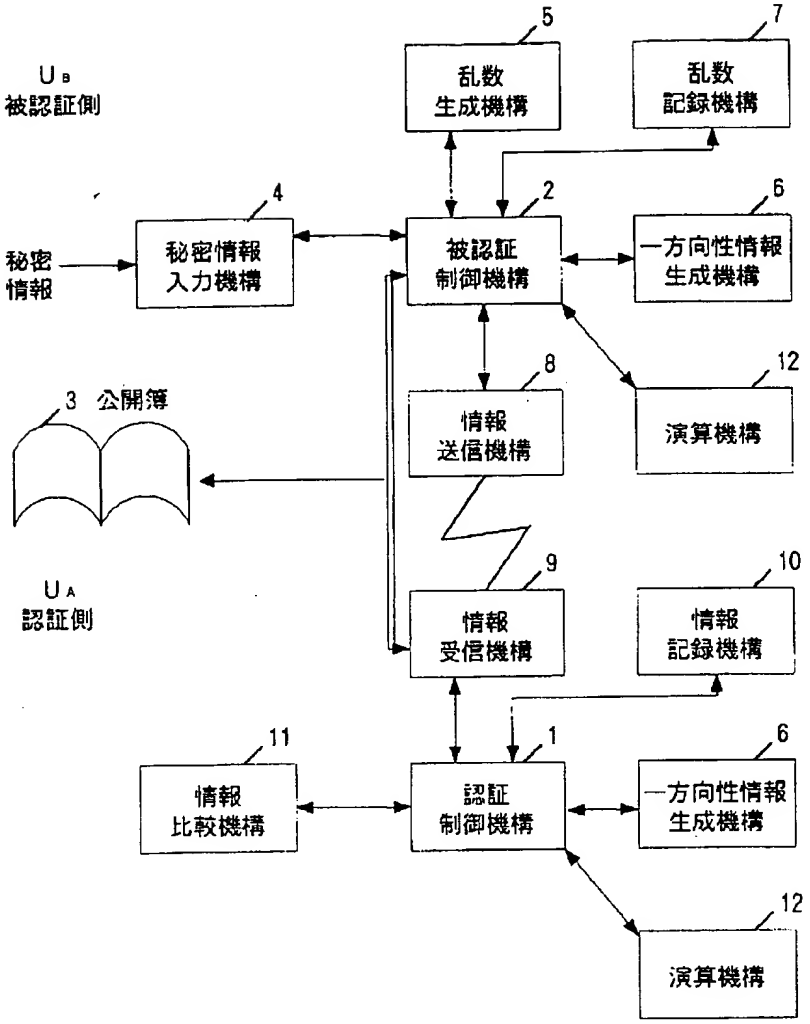

被認証者U_B
(ユーザID＝A、パスワード＝S)
認証者U_A
乱数$N_{(1)}$を生成、記憶
$E_{(1)} \leftarrow E(A, S@N_{(1)})$
$E^2_{(1)} \leftarrow E(A, E_{(1)})$
$E_{(0)} \leftarrow E(A, S@N_{(0)})$
$E^2_{(0)} \leftarrow E(A, E_{(0)})$
$F_{(0)} = E_{(0)} @ E^2_{(0)}$
$G_{(1)} = E^2_{(1)} @ E^2_{(0)}$
A, $F_{(0)}$, $G_{(1)}$を一般ルートで通知
$X = F_{(0)} @ Z$
$Y \leftarrow E(A, X)$
Y＝Z？
No
Yes
認証不成立
認証成立：
$Z' = G_{(1)} @ Z$
Z'をU_Bの新しい認証パラーメータ
Z（次回認証用）として記憶

【図３】

［第ｋ回目の認証フェーズ］



【図４】



フロントページの続き

(72)発明者　栗原　定見
東京都武蔵野市御殿山一丁目１番３号　エヌ・ティ・ティ・アドバンステクノロジ株式会社内

Ｆターム(参考)　5B085 AE09 AE23
5J104 AA07 JA13 JA14 KA01 NA05
NA11 PA07